Table des matières#

1. INTRODUCTION

1.1. Help Channel Burundi (HCB) and together with his partners has a commitment to high legal, ethical and moral standards. All employees of HCB are expected to share this commitment.

1.2. Fraud is an issue that all organizations may face regardless of size, industry or country. HCB takes a zero-tolerance attitude to fraud and will uphold all applicable laws relevant to countering fraud in all jurisdictions in which it operates.

1.3. The Executive Committee of the Organization (hereinafter *the Board)* carries out overall responsibility to ensure that risk culture is established, and fraud awareness is continuously raised within HCB. Fraud is an ever-present threat and hence must be a concern to all employees. The organization views fraud as an extremely serious matter and is committed to continuous promotion of anti-fraud culture throughout the organization.

1.4. The purpose of this Anti-Fraud Policy (hereinafter *the Policy)* is to provide an overall framework for a response, advice and direction to those who find themselves having to deal with suspected cases of fraud.
1.5. The Policy applies to any suspected or accomplished irregularity, involving employees as well as consultants, vendors, contractors, and/or any other external parties having a business relationship with the organization.
1.6. Any investigative activity required will be conducted without regard to any person's relationship to HCB, position or length of service. All employees have a duty to familiarize themselves with the types of improprieties that might be expected to occur within their areas of responsibility and to be alert to any indications ("red flags") of fraud risk.

1.7. The Policy is supplemented by the "Policy on reporting allegations of suspected improper activities" (hereinafter *the "Whistleblowing" Policy)* providing a procedure for reporting information related to alleged or suspected Improper Activities, by the "Policy on Investigation of Improper Activities" governing overall investigation process related to any suspected or alleged improper activity within the organization, and "Help Channel Burundi Anti-Corruption Policy" focusing on bribery and improper payments to gain influence or benefit advantage in return.

2. DEFINITIONS – WHAT IS FRAUD?

2.1. Fraud is defined1 as "any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by persons to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage." The term “fraud” commonly includes activities such as theft, corruption, conspiracy, embezzlement, money laundering, deception, bribery, abuse of authority, insider dealing and extortion. It may involve:

(i) Manipulation, falsification or adjustments of records or documents;

(ii) Suppression or omission of the effects of transactions from records or documents;

(iii) Recording of transactions without substance;

(iv) Asset misappropriation or wellful destruction, including theft of cash or other assets (suppliers, inventory, equipment, and information);

(v) Undisclosed personal economic interest (conflict of interest) in a transaction that adversely affects the organization or its shareholders;

(vi) Offering, giving, receiving, or soliciting anything of value to influence an outcome;

(vii) Provision of unreasonable donations to fake charity organizations;

(viii) Deliberate misapplication of accounting or other regulations or policies.

2.2. The criminal act is the attempt to deceive, and attempted fraud is therefore treated as seriously as accomplished fraud.

2.3. Computer fraud arises where information technology equipment has been used to manipulate program applications or data dishonestly (for example, by altering, substituting or destroying records, or creating spurious records), or where the use of an IT system was a material factor in perpetration of fraud (for example, unauthorized access to relevant systems, overriding systems of controls). Theft or fraudulent use of computer time and resources is included in this definition.

2.4. Some illustrations of incidents which would be classified as fraud are contained in Appendix A to this Policy.

3. MANAGING THE RISK OF FRAUD - RESPONSIBILITIES

3.1. Each office of the Organization must establish proactive approach to fraud risk management via sustaining and continuously promoting zero-tolerance attitude towards fraud, promulgating fraud awareness culture among all employees.
3.2. Each office of the organization must initiate and undertake an investigation where there is suspected fraud and take appropriate legal and/or disciplinary action in all cases where that would be justified. Where there is fraud (suspected or proven), each office of the Organization should make any necessary changes to existing Internal Control Framework (i.e. systems and procedures) to ensure prevention of any future occurrence of similar fraud. Each office of the Organization should also establish system for recording and subsequently monitoring all discovered cases of fraud (suspected or proven) and the effectiveness of corrective measures implemented.
3.3. Overall responsibility for managing the risk of fraud has been assigned to the Executive Management (hereinafter *the Management Team*) and the Heads of Functions (i.e. Directors, Heads of Departments).
3.4. Responsibility for exercising disciplinary actions, as consequence management, rests with the Human Resources department (or similar position), where appropriate in consultation with the Management Team.

3.5. The **Executives** are responsible for overall management of fraud risk, including:

- establishing and maintaining sound systems of risk management and internal control that support the achievement of organization's strategy;
- defining a fraud risk profile and undertaking a regular review of the fraud risks associated with each of the key organizational objectives to keep the profile up to date;
- establishing appropriate mechanisms for reporting issues related to fraud risk;
- ensuring development of a system for prompt, competent, and confidential review, investigation, and resolution of instances of noncompliance and allegations involving potential fraud;
- ensuring that all employees are aware of the HCB's overall attitude to fraud and their individual responsibilities in relation to combating fraud;
- ensuring that appropriate anti-fraud training and development opportunities are available to the employees;
- choosing appropriate consequence management towards employees committing fraud;
- ensuring that appropriate actions are taken to safeguard the recovery of assets;

- ensuring that efficient and economically sound actions are taken to prevent future recurrence of similar frauds;
- ensuring there is a process for tracking and case management where all allegations of fraud are logged

3.6. **Heads of Functions** have overall responsibility for preventing, detecting and managing the fraud risk on a day to day basis, including:

- identifying and assessing of fraud risks to which systems, operations and procedures within their area of accountability are exposed;
- designing, developing and maintaining effective system of internal control which ensures prevention and timely detection of fraud risks;
- ensuring that established internal controls are being continuously complied with and relevant systems continue to operate effectively;
- Regularly reviewing and testing controls in place, questioning the adequacy, relevance and robustness of the overall system of internal control, and, where appropriate, implementing new controls to reduce the risk of similar fraud occurrence in the future.

3.7. Every **employee** is responsible for:

- acting with propriety in the use of HCB's resources and the handling and usage of funds whether they are involved with cash or payments systems, receipts or dealing with suppliers or customers;
- being conscious to the possibility that unusual events or one-off transactions could be indicators of potential fraud;
- immediately reporting details of suspected fraud or irregularity through the established information channel in accordance with HCB's Policy on Reporting Allegations of Suspected Improper Activities (hereinafter *the "Whistleblowing Policy"*);
- Co-operating fully with dedicated employees assigned to conduct internal checks, reviews or fraud investigations.

3.8. Responsibilities of **Internal Auditor** include:

- delivering an opinion to the Executives and the Audit and Risk Committee, to whom the Board discharged its governance and control function over the systems of risk management and internal control, on the adequacy of

arrangements for managing the risk of fraud and ensuring that the Organization promotes and sustains anti-fraud culture;
- assisting in the deterrence and prevention of fraud by examining and evaluating the effectiveness and efficiency of internal controls commensurate with the extent of the potential exposure/risk in the various segments of HCB's business;
- Assisting Management in conducting fraud investigations. 3.9. Responsibilities of the **Audit and Risk Committee** include:

3.9. Responsibilities of the **Audit and Risk Committee** include:

- ensuring there is due process for the identification and management of fraud risks to encourage ethical behaviour and zero-tolerance attitude to fraud;
- monitoring HCB's procedure for the safeguarding of its assets and ensuring the Organization has adequate policies in place for the prevention and detection of fraud;
- Reviewing procedures established within the Organization by which employees may, in confidence, report an allegation regarding potential or actual fraud incident.

4. FRAUD RESPONSE

To ensure that effective and timely action is taken in a professional manner to any suspected or proved fraud or any other irregularity, the Organization has established an overall response procedure which defines the steps to be followed in such cases.

4.1. Fraud Detection

Every employee may come across indicators of potential fraud in the due course of daily operational activity. As an example, unusual events or one-off transactions as well as any unintentional incident or action, which is not part of the normal operation of the system or the expected course of actions and events, could be indicators of potential fraud. All employees should be alert to the possibility of fraud and ensure timely reporting about any suspicious indicators discovered.

Fraud may also be highlighted as a result of specific and/or unscheduled management checks or be brought to management's attention by a third party. Additionally, irregularities occasionally come to light in the course of audit engagements.

4.2. Reporting

When an employee suspects that a fraud or irregularity has occurred, he/she should notify his/her immediate Supervisor or other appropriate Management Team member (in case the immediate Supervisor is involved) and Internal Auditor immediately.
The overall procedure for reporting information is defined in accordance with the Organization's Policy on reporting allegations of suspected improper activities.
Speed is of the essence and such initial report can be verbal and must be followed up within 24 hours by a written report addressed which should cover:

a) the amount/value, if established;
b) the position regarding recovery;
c) the period over which the fraud or irregularity occurred, if known;
d) the date of discovery and how the suspected fraud or irregularity was discovered;
e) whether the person responsible has been identified;
f) whether any collusion with others is suspected;
g) details of any actions taken to date;
h) any other information or comments which might be relevant

In case any question or concern raised with respect to further course of actions required, it is reasonable for the reporting employee to apply for further consultation to Internal Auditor of the Organization.

4.3. Investigation/Further Actions

A preliminary review will be conducted with respect to any allegation of potential fraud to validate the suspicion raised and assess whether the case is substantiated enough to start the investigation process.
The Organization is committed to perform comprehensive analysis of all factors, which gave rise to the suspicion of potential improper activity to conclude whether a genuine mistake has been made or irregularity has occurred.
The preliminary review and consequent investigation will be organized and performed strictly in accordance with the established procedure defined in the "Policy on investigation of improper activities" of the Organization in a timely manner. **Prompt action is an essential aspect**.

Upon the completion of the investigation the Organization and each office of the Organization will determine the course of actions to be taken, including application of the required legal and disciplinary measures, in all the cases which deemed to be appropriate.

The Organization may, for example, incorporate changes to the existing internal control framework (business process re-engineering, incorporation of IT systems, development of internal policies and procedures) to prevent occurrence of similar cases in the future.

Information on all allegations regarding suspected or proved Improper Activities will be maintained in the corporate case-tracking system. The data logged in the system will contain the executive summary of the results of all the conducted investigation and all consequence management in case organized.

5. LEARNING FROM EXPERIENCE

5.1. Capturing lessons learned is a vital element of the overall anti-fraud culture promulgated within HCB. In order to provide a deterrent to other personnel and to prevent future recurrence of the fraud a brief and anonymized summary of the circumstances may be published and distributed within the office of the Organization to share the information on the lessons learned.

5.2. Examples of unacceptable behaviour and business conduct following lessons learned from the fraud cases investigations are regularly incorporated (whether relevant) into induction training as part of the on boarding process for all newly arrived employees.

APPENDIX A

WHERE MIGHT FRAUD HAPPEN?

Fraud can happen wherever employee, partnering organization or independent contractors complete official documentation and can take financial advantage of the Office of the organization. The risk of fraud is enhanced where employees or contractors are in positions of trust or responsibility and are not checked or subjected to effective monitoring or validation.

There are various frauds schemes used by perpetrators. As an example, below several types of internal fraud are provided:

(1) Asset misappropriation:

(a) Cash:

(i) ***Theft of cash:*** stealing money from petty cash;

(ii) ***False payments:*** employee creating false payments instructions with forged signatures and submitting it for processing;

(iii) ***Billing schemes:*** over billing customers; recording of false credits, rebates or refunds to customers; pay and return schemes; using fictitious suppliers or shell companies for false billing;

(iv) ***Misuse of accounts:*** unrecorded sales or receivables; employee account fraud (where an employee is also a customer, and employee makes unauthorized adjustments to their accounts)

(b) Non-cash:

(i) ***Inventory and fixed assets:*** theft of inventory; false write offs and other debits to inventory accounts; false sale of inventory; theft of fixed assets including computers and other IT related assets; receiving free or below market value or goods from suppliers; unauthorized private use of corporate property; theft or abuse of proprietary or other confidential information (customer information, intellectual property; pricing schedules, etc.);

(ii) ***Contracting and procurement:*** falsifying documents to obtain authorization for payment; forging signatures on payment authorization; submitting false invoices for payment or from fictitious suppliers; sending fictitious or duplicate invoices to suppliers; mark-up invoices from contracts awarded to suppliers associated with employees; intercepting payments to suppliers; sale of critical bid information, contract details or other sensitive information; improper change to supplier's payment terms or other details;

(iii) ***Payroll:*** fictitious (ghost) employees on the payroll; falsifying work hours to achieve fraudulent overtime payments; abuse of commission schemes; improper changes in salary levels; abuse of holiday leave or time off entitlements; submitting inflated or false expense claims; adding private expenses to legitimate expense claims; applying of multiple reimbursement of the same expenses; false workers' compensation claims

Examples of Internal Fraud include, but not limited to the below presented:

2) Fraudulent Statements:

Financial:

(i) ***Improper revenue recognition:*** holding the books open after the end of the accounting period; inflation of sales figures which are credited out after the year end; backdating agreements; improper classification of revenues; recording fictitious sales and shipments; inappropriate estimation of returns, price adjustments and other concessions; over/under estimation of work completed under long-term contracts; incorrect inclusion of related part receivables, etc.

(ii) ***Misstatement of assets, liabilities and/or expenses:*** fictitious fixed assets; overstating assets acquired (through mergers and acquisitions); incorrect value attached to goodwill; manipulation of fixed assets valuation; off balance sheet items; delaying recording the expenses to the next accounting period, etc.;

(iii) ***Other accounting misstatements:*** improper treatment of inter-organization accounts; non-clearance or improper clearance of suspense accounts; fictitious general ledger accounts; journal entry fraud; improper or inadequate disclosures, etc.;

(a) *Non-financial***,** include falsified employment credentials (e.g. qualifications and references) and other fraudulent internal or external documents.

(3) Corruption:

(a) conflict of the interests:

(i) ***Kickbacks:*** kickback to employees by a supplier in return for a supplier receiving favorable conditions; purchase of a property at a price higher than market value in exchange of the kickback; preference treatment of a customer in exchange for a kickback, etc.;

(ii) ***Personal interest:*** collusions with customers/suppliers; favoring a supplier in which an employee has financial interest; transfer of knowledge to a competitor by an employee who intends to join the competitor's organization; insider trading; etc.;

(b) Bribery and extorsion:

(i) ***Bribery:*** payment of agency/facilitation payment in order to secure a contract; authorizing orders to a particular supplier in return for bribes; giving and accepting payment to favor/not to favor other commercial transactions or relationships; anti-trust activities, such as price fixing or bid rigging, etc.;

(ii) ***Extortion:*** blackmail (offering to keep information confidential in return for money or other consideration); extortion (offering to keep someone from harm in return for money or other consideration).

Policy Approval by the Board of Directors.
Date approved: 16/3/2018